APPENDIX A

CLAIM AMENDMENTS RELATIVE TO THE SUBMISSION OF 6/8/2005

1. (Currently amended) A method for communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the steps of:

developing k distinct random prime numbers $p_1, p_2, \ldots, p_k$, wherein k is an integer greater than 2;

providing a number e relatively prime to $(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)$;

providing a composite number n equaling the product $p_1\cdot p_2\cdot\ldots\cdot p_k$;

receiving a ciphertext word signal C which is formed by encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of the message and

$$0 \le M \le n-1$$

where C is a number representative of an encoded form of the plaintext message word signal M such that

$$C \equiv M^e \pmod{n}$$

and where e is associated with an intended recipient of the ciphertext word signal C; and

deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime number $p_1, p_2, \ldots p_k$;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the deciphering step if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a deciphering step if the pair of prime numbers p and q is used instead.

2. (Previously presented) The method according to claim 1, wherein the deciphering step includes

establishing a number, d, as a multiplicative inverse of e(mod(lcm((p_1–1), (p_2–1), . . . (p_k–1)))), and

decoding the ciphertext word signal C to the plaintext message word signal M where $M \equiv C^d \pmod{n}$.

3. (Currently amended) A method for communications of a message signal M_i cryptographically processed with RSA public key encryption in a system having j terminals, each terminal being characterized by an encoding key $E_i = (e_i, n_i)$ and a decoding key $D_i = (d_i, n_i)$, where i = 1, 2, . . . , j, and the message signal M_i corresponds to a number representative of a message-to-be-received from the i^{th} terminal, the method comprising the steps of:

establishing n_i where n_i is a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$$

where k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to ~~lcm($p_{i,1}$–1, $p_{1,2}$–1, $p_{i,k}$–1)~~lcm($p_{i,1}$–1, $p_{i,2}$–1, . . . , $p_{i,k}$–1), and

d_i is selected from the group consisting of ~~the~~ a class of numbers equivalent to a multiplicative inverse of

$$e_i(\text{mod}(\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))));$$

receiving by a recipient terminal (i = y) from a sender terminal (i = x, x ≠ y) a ciphertext signal C_x formed by encoding a digital message word signal M_x, wherein the encoding includes

transforming said message word signal M_A to one or more message block word signals M_x", each block word signal M_x" corresponding to a number representative of a portion of said message word signal M_x in the range $0 \leq M_x" \leq n_y-1$, and

transforming each of said message block word signals M_x" to a ciphertext word signal C_x that corresponds to a number representative of an encoded form of said message block word signal M_x" where ~~$C_x \equiv M_A"^{ey} \pmod{n_y}$~~

$$C_x \equiv M_x"^{e_y} \pmod{n_y}; \text{ and}$$

deciphering the received ciphertext word signal C_x at the recipient terminal having available to it the k distinct random prime numbers $p_{y,1}$, $p_{y,2}$, ..., $p_{y,k}$ for establishing its d_y;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the deciphering step if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a deciphering step if the pair of prime numbers p and q is used instead.

4. (Currently amended) A system for communications of a message cryptographically processed with an RSA public key encryption, comprising:

a communication channel for transmitting a ciphertext word signal C;

encoding means coupled to said channel and adapted for transforming a transmit message word signal M to the ciphertext word signal C using a composite number, n,

where n is a product of the form

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k,$$

k is an integer greater than 2, and p_1, p_2, . . . , p_k are distinct random prime numbers,

where the transmit message word signal M corresponds to a number representative of the message and $0 \leq M \leq n-1$,

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$$C \equiv M^e \pmod{n}, \text{ and}$$

where e is a number relatively prime to $\text{lcm}(p_1-1, p_2-1, \ldots, p_k-1)$; and

decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and, having available to it the k distinct random prime numbers p_1, p_2, . . . p_k, for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a decoded form of the ciphertext word signal C through a relationship of the form

$$M' \equiv C^d \pmod{n}$$

where d is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

$$e(\mathrm{mod}(\mathrm{lcm}((p_1-1), (p_2-1), \ldots, (p_k-1))));$$

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein transforming the ciphertext word signal C to a receive message word signal M' is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the transforming of the ciphertext word signal C if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a transforming of the ciphertext word signal C if the pair of prime numbers p and q is used instead.

5. (Currently amended) A system for communications of a message cryptographically processed with an RSA public key encryption, the system having a plurality of terminals coupled by a communications channel, comprising:

a first terminal of the plurality of terminals characterized by an encoding key $E_A = (e_A, n_A)$ and a decoding key $D_A = (d_A, n_A)$,

where n_A is a composite number of the form

$$n_A = p_{A,1} \cdot p_{A,2} \cdot \ldots \cdot p_{A,k}$$

where

k is an integer greater than 2,

$p_{A,1}$, $p_{A,2}$, . . . , $p_{A,k}$ are distinct random prime numbers,
e_A is relatively prime to

lcm($p_{A,1}$–1, $p_{A,2}$–1, . . . , $p_{A,k}$–1), and

d_A is selected from the group consisting of ~~the~~ a class of numbers equivalent to a multiplicative inverse of

e_A (mod(lcm(($p_{A,1}$–1), ($p_{A,2}$–1), . . . , ($p_{A,k}$–1)))); and

a second terminal of the plurality of terminals having

blocking means for transforming a first message, which is to be transmitted on said communications channel from said second terminal to said first terminal, into one or more transmit message word signals M_B, where each M_B corresponds to a number representative of said first message in the range

$0 \leq M_B \leq n_A$–1, and

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that corresponds to a number representative of an encoded form of said first message through a relationship of the form

~~$C_B \equiv M_B^{eA} (\text{mod} n_A)$~~ $C_B \equiv M_B^{e_A} (\text{mod} n_A)$,

said first terminal having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_B from said channel and, having available to it the k distinct random prime numbers $p_{A,1}$, $p_{A,2}$, . . . $p_{A,k}$,

for transforming each of said ciphertext word signals C_B to a receive message word signal ~~M'$_B$~~ M_B', and

means for transforming said receive message word signal ~~M'$_B$~~ M_B' to said first message, where ~~M'$_B$~~ M_B' corresponds to a number representative of a decoded form of C_B through a relationship of the form

$$~~M'_B \equiv C_B^{dA} (\mathrm{mod}\, n_A)~~ M_B' \equiv C_B^{d_A} (\mathrm{mod}\, n_A);$$

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein transforming said receive message word signal M_B' to said first message is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the transforming of said receive message word signal M_B' if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a transforming of said receive message word signal M_B' if the pair of prime numbers p and q is used instead.

6. (Currently amended) The system according to claim 5 wherein said second terminal is characterized by an encoding key $E_B = (e_B, n_B)$ and a decoding key $D_B = (d_B, n_B)$, where

n_B is a composite number of the form

$$n_B = p_{B,1} \cdot p_{B,2} \cdot \ldots \cdot p_{B,k},$$

where

k is an integer greater than 2,

$p_{B,1}, p_{B,2}, \ldots, p_{B,k}$ are distinct random prime numbers,

e_B is relatively prime to

$$\text{lcm}(p_{B,1}-1, p_{B,2}-1, \ldots, p_{B,k}-1), \text{ and}$$

d_B is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

$$e_B \ (\text{mod}(\text{lcm}((p_{B,1}-1), (p_{B,2}-1), \ldots, (p_{B,k}-1))))$$

said first terminal further having

blocking means for transforming a second message, which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A, where each M_A corresponds to a number representative of said message in the range

$$0 \leq M_A \leq n_B-1, \text{ and}$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, where C_A corresponds to a number representative of an encoded form of said second_message through a relationship of the form

~~$C_A \equiv M_A^{eB} (\text{mod} n_B)$~~ $C_A \equiv M_A^{e_B} (\text{mod} n_B)$; and

said second terminal further having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_A from said channel and, having available to it the k distinct random prime numbers $p_{B,1}$, $p_{B,2}$, . . . , $p_{B,k}$, for transforming each of said ciphertext word signals to a receive message word signal ~~M'$_A$~~ M_A', and

means for transforming said receive message word signals ~~M'$_A$~~ M_A' to said second message, where ~~M'$_A$~~ M_A' corresponds to a number representative of a decoded form of C_A through a relationship of the form

$$\text{~~}M'_A \equiv C_A^{dB} (\text{mod } n_B)\text{~~}\ M_A' \equiv C_A^{d_B} (\text{mod } n_B).$$

7. (Canceled).

8. (Canceled).

9. (Currently amended) A system for communications of message signals cryptographically processed with RSA public key ~~encryption~~signing, comprising:

j terminals including first and second terminals, each of the j terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where i = 1, 2, . . . ,j, each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is transmitted from an i^{th} terminal and

$$0 \leq M_i \leq n_i - 1,$$

n_i being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}$, $p_{i,2}$, . . . , $p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to lcm($p_{i,1}$–1,$p_{i,2}$–1, . . . , $p_{i,k}$–1), and

d_i is selected from the group consisting of ~~the~~ a class of numbers equivalent to a multiplicative inverse of

$$e_i \,(\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))));$$

said first terminal including

means for encoding a digital message word signal M_1 to be transmitted from said first terminal (i=1) to said second terminal (i=2), said encoding means transforming said digital message word signal M_1 to a signed message word signal M_{1s} using a relationship of the form

~~$M_{1s} \equiv M_1^{d1} (\mathrm{mod}\, n_1)$~~ $M_{1s} \equiv M_1^{d_1} (\mathrm{mod}\, n_1)$; and

means for transmitting said signed message word signal M_{1s} from said first terminal to said second terminal, wherein said second terminal includes

means for decoding said signed message word signal M_{1s} to said digital message word signal M_1;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime number each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein encoding a digital message word signal M_1 is divided into sub-steps, on sub-step for each of the k distinct random prime numbers; and

wherein for a give number of digits for composite numbers n and m, it takes fewer computational cycles to perform the encoding of the digital message word signal M_1 if the k distinct random prime numbers are

used, relative to the number of computational cycles for performing an encoding of the digital message word signal M_1 if the pair of prime numbers p and q is used instead.

10. (Currently amended) The system of claim 9, wherein the means for decoding signed message word signal ~~M_{As}~~ M_{1s} includes means for transforming said signed message word signal ~~M_{As}~~ M_{1s} to said digital message word signal M_1 using a relationship of the form ~~$M_1 \equiv M_1^{e1} (\mathrm{mod}\, n_1)$~~ $M_1 \equiv M_{1s}^{e_1} (\mathrm{mod}\, n_1)$.

11. (Currently amended) A communications system for transferring a message signal cryptographically processed with RSA public key encryption, the communications system comprising:

j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key $E_i = (e_i, n_i)$ and a decoding key $D_i = (d_i, n_i)$, where i = 1, 2, . . . , j, each of the j communication stations being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is received from an i^{th} communication station, and

$$0 \le M_i \le n_i - 1$$

n_i being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\mathrm{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots, p_{i,k}-1)$, and

d_i is selected from the group consisting of ~~the~~ a class of numbers equivalent to a multiplicative inverse of

$$e_i \ (\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))))_1$$

said first station including

means for encoding a digital message word signal M_1 to be transmitted from said first station (i =1) to said second station (i = 2),

means for transforming said digital message word signal M_1 to one or more message block word signals M_1", each block word signal M_1" being a number representative of a portion of said digital message word signal M_1 in the range

$0 \leq M_1" \leq n_2-1$, and

means for transforming each of said message block word signals M_1" to a ciphertext word signal ~~C1~~ C_1 using a relationship of the form

~~$C_1 \equiv M_1"^{e2} (\mathrm{mod} n_2)$~~ $C_1 \equiv M_1"^{e_2} (\mathrm{mod} n_2)$; and

means for transmitting said ciphertext signals C_1 from said first station to said second station, wherein said second station includes

means for deciphering said ciphertext signals C_1 using $p_{2,1}$, $p_{2,2}$, . . . $p_{2,k}$ to produce said digital message word signal M_1;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein deciphering said ciphertext signals C_1 is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the deciphering of said ciphertext signals C_1 if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a deciphering of said ciphertext signals C_1 if the pair of prime numbers p and q is used instead.

12. (Currently amended) The communications system of claim 11, wherein the deciphering means includes

means for decoding said ciphertext word signals C_1 to said message block word signals M_1" using a relationship of the form

~~$M_1" \equiv C_1^{d2} (\mathrm{mod}\, n_2)$~~ $M_1" \equiv C_1^{d_2} (\mathrm{mod}\, n_2)$, and

means for transforming said message block word signals M_1" to said message word signal M_1.

13. (Canceled).

14. (Currently amended) A method of communicating a message cryptographically processed with an RSA public key encryption, comprising the steps of:

selecting a public key portion e associated with a recipient intended for receiving the message;

developing k distinct random prime numbers, p_1, p_2, . . . p_k, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1–1, p_2–1, . . . p_k–l, is relatively prime to the public key portion e;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message formed by encoding a plaintext message data M to the ciphertext message data C using a relationship of the form

$C \equiv M^e \pmod{n}$

where M represents the message, where $0 \leq M \leq n-1$, and where the sender knows n and the public key portion e but has no access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$; and

deciphering at the recipient the received ciphertext message data C to produce the message, the recipient having access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the deciphering step if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a deciphering step if the pair of prime numbers p and q is used instead.

15. (Previously presented) The method according to claim 14, comprising the further step of:

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

wherein the deciphering step includes decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

16. (Currently amended) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers p_1, p_2, . . . p_k, where k ≥ 3, and checking that each of the k distinct random prime numbers minus 1, p_1–1, p_2–1, . . . p_k–l, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message data C representing an encoded form of a plaintext message data M: and

decoding the received ciphertext message data C to the plaintext message data M using a relationship of the form

$$M \equiv C^d \ (\mathrm{mod}\ n),$$

the decoding performed by a recipient owning the private key portion d and having access to the k distinct random prime numbers p_1, p_2, . . . p_k;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein the decoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the decoding step if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a decoding step if the pair of prime numbers p and q is used instead.

17. (Previously presented) The method according to claim 16, wherein the ciphertext message data C is formed by encoding the plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, wherein $0 \leq M \leq n-1$ and wherein n and the public key portion e are accessible to the sender although it has no access to the k distinct random prime numbers $p_1, p_2, \ldots p_k$.

18. (Currently amended) A method of communicating a message cryptographically processed with RSA public key ~~encryption~~signing, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1} \pmod{((p_1-1)\cdot(p_2-1)\cdots(p_k-1))}$;

computing a composite number, n, as a product of the k distinct random prime numbers;

encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form

$$M_s \equiv M^d \pmod{n},$$

where $0 \leq M \leq n-1$;

receiving the signed message M_s; and

deciphering the signed message to produce the plaintext message data M;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the encoding step if the k distinct random prime numbers are used, relative to the number of computational cycles for performing an encoding step if the pair of prime numbers p and q is used instead.

19. (Previously presented) The method of claim 18, wherein the deciphering step includes:

decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

20. (Currently amended) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

sending to a recipient a cryptographically processed message formed by assigning a number M to represent the message in plaintext message form, and cryptographically transforming the assigned number M from the plaintext message form to a number C that represents the message in an encoded form, wherein the number C is a function of

the assigned number M,

a number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e having been obtained by the sender are associated with the recipient to which the message is intended; and

receiving the cryptographically processed message which is decipherable by the recipient based on

the number n,

another exponent d, and

the number C,

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the at least three distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein deciphering the cryptographically processed message is divided into sub-steps, one sub-step for each of the at least three distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the deciphering if the at least three distinct random prime numbers are used, relative to the number of computational cycles for performing a deciphering if the pair of prime numbers p and q is used instead.

21. (Previously presented) The method according to claim 20,

wherein the cryptographically transforming step includes using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers $p_1, p_2, \ldots p_k$, using a relationship of the form $d \equiv e^{-1} \pmod{((p_1-1)\cdot(p_2-1)\cdots(p_k-1))}$, and

wherein the cryptographically processed message is deciphered using a relationship of the form $M \equiv C^d \pmod{n}$.

22. (Currently amended) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

receiving from a sender a cryptographically processed message, in the form of a number C, which is decipherable by the recipient based on a number n, an exponent d, and the number C; and

deciphering the cryptographically processed message,

wherein a number M represents a plaintext form of the message,

wherein the number C represents a cryptographically encoded form of the message and is a function of

the number M,

the number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e are associated with the recipient to which the message is intended, and

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the at least three distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein deciphering the cryptographically processed message is divided into sub-steps, one sub-step for each of the at least three distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the deciphering if the at least three distinct random prime numbers are used, relative to the number of

computational cycles for performing a deciphering if the pair of prime numbers p and q is used instead.

23. (Previously presented) The method according to claim 22,

wherein the number C is formed using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers p_1, p_2, . . . p_k, using a relationship of the form $d \equiv e^{-1}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

and wherein the number M is obtained using a relationship of the form $M \equiv C^d \pmod{n}$.

24. (Canceled).

25. (Canceled).

26. (Canceled).

27. (Canceled).

28. (Canceled).

29. (Canceled).

30. (Canceled).

31. (Canceled).

32. (Canceled).

33. (Canceled).

34. (Currently amended) The method according to claim 14, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by **[[n]]** the composite number m being ~~equal to a composite number~~ computed as the product of **[[2]]** the pair of prime numbers p and q, is decipherable with multi-prime (k > 2) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers p_1, p_2, . . . p_k.

35. (Currently amended) The method according to claim 9, wherein the signed message word signal M_{1s}, formed from the digital message word signal M_1 being cryptographically processed at the first terminal with multi-prime (k > 2) RSA public key ~~encryption~~ signing which is characterized by the composite number n being computed as the product of the k distinct random prime numbers p_1, p_2, . . . p_k, is decipherable at the second terminal with two-prime RSA public key ~~encryption~~ signing characterized by **[[n]]** the composite number m being ~~equal to a composite number~~ computed as the product of **[[2]]** the pair of prime numbers p and q.

36. (Currently amended) The method according to claim 16, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by **[[n]]** the composite number m being ~~equal to a composite number~~ computed as the product of **[[2]]** the pair of prime numbers p and q, is decipherable by the decoding with multi-prime (k > 2) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers p_1, p_2, . . . p_k.

37. (Currently amended) The method according to claim 18. wherein the signed message M_s formed from the plaintext message data M being cryptographically processed at the sender with multi-prime (k > 2) RSA public key signing which is characterized by the composite number n being computed as the product of the k distinct random prime numbers p_1, p_2, . . . p_k, is

decipherable by the decoding at the recipient with two-prime RSA public key signing characterized by **[[n]]** the composite number m being ~~equal to a composite number~~ computed as the product of **[[2]]** the pair of prime numbers p and q.

38. (Currently amended) The method according to claim 20, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by **[[n]]** the composite number m being ~~equal to a composite number~~ computed as the product of **[[2]]** the pair of prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

39. (Currently amended) The method according to claim 22. wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by **[[n]]** the composite number m being ~~equal to a composite number~~ computed as the product of **[[2]]** the pair of prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

40. (Currently amended) A cryptography method for local storage of data by a private key owner, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers p_1, p_2, . . . p_k, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers that are factors of n, where only the private key owner knows the factors of n; and

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form

$$C \equiv M^e \pmod{n},$$

wherein $0 \leq M \leq n-1$, whereby the ciphertext data C is decipherable only by the private key owner having available to it the factors of n;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the encoding step if the k distinct random prime numbers are used, relative to the number of computational cycles for performing an encoding step if the pair of prime numbers p and q is used instead.[[.]]

41. (Previously presented) The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod{n}$.

42. (Currently amended) A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to communicate with the plurality of stations via the communications medium sending [[a]] and receiving messages cryptographically processed with an RSA public key encryption, the host system including at least one cryptosystem configured for

developing k distinct random prime numbers p_1, p_2, . . . , p_k, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship of the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

in response to an encoding request from the host system, encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form

$$C \equiv M^e \pmod{n}, \text{ where } 0 \leq M \leq n-1, \text{ and}$$

in response to a decoding request from the host system, decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form

$$M' \equiv C'^d \pmod{n};$$

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein decoding the ciphertext message data C' is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the decoding of the ciphertext message data C' if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a decoding of the ciphertext message data C' if the pair of prime numbers p and q is used instead.

43. (Currently amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem communicatively coupled to and receiving from the bus encoding and decoding requests, the cryptosystem being configured for

providing a public key portion e,

developing k distinct random prime numbers p_1, p_2, . . . p_k, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

in response to an encoding request from the bus, encoding a plaintext form of a first message M to produce C, a ciphertext form of the first message, using a relationship of the form

$$C \equiv M^e \pmod{n},$$

where $0 \leq M \leq n-1$, and

in response to a decoding request from the host system, decoding C', a ciphertext form of a second message, to produce M', a plaintext form of the second message, using a relationship of the form

$$M' \equiv C'^{d} \pmod{n},$$

the first and second messages being distinct or one and the same;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein decoding C' is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the decoding of C' if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a decoding of C' if the pair of prime numbers p and q is used instead.

44. (Previously presented) The system of claim 42, wherein the at least one cryptosystem includes

a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. (Currently amended) The system of claim 42, wherein the at least one cryptosystem includes

a processor,

a data-address bus,

a memory coupled to the processor via the data-address bus,

a data encryption standard (DES) unit coupled to the memory and the processor via the data-address bus, and

a plurality of exponentiator elements coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. (Previously presented) The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that cryptographically processes message data received/returned from/to the processor.

47. (Previously presented) The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor, including secure, insecure and exponentiator elements address spaces, and wherein the DES unit is configured to recognize the secure and exponentiator elements address spaces and to automatically encode message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when the processor is accessing the insecure memory address spaces, the DES unit being further configured to decode encoded message data received from the memory before it is provided to the processor.

48. (Previously presented) The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. (Previously presented) The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors $p_1, p_2, \ldots p_k$.

50. (Currently amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding request providing a plaintext message M to be encoded,

obtaining a public key that includes an exponent e and a modulus n, a representation of the modulus n existing in the memory in the form of its k distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$,

constructing subtasks, one subtask for each of the k factors, to be executed by the exponentiator elements for producing respective ones of the subtask values $C_1, C_2, \ldots C_k$, and

forming a ciphertext message C from the subtask values $C_1, C_2, \ldots C_k$,

wherein the ciphertext message C is decipherable using a private key that includes the modulus n and an exponent d which is a function of e;

wherein p and q are a pair of prime numbers that product of which equals a modulus m, the k distinct random prime numbers each smaller than p and q, and the modulus m having the same number of digits as the modulus n; and

wherein for a given number of digits for modulus n and modulus m, it takes fewer computational cycles to form the ciphertext message C if the k distinct random prime numbers are used, relative to the number of computational cycles for forming a ciphertext message C' if the pair of prime numbers p and q is used instead.

51. (Currently amended) The system of claim 50, wherein each one of the subtask values C_1, C_2, . . . C_k is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\text{mod } p_i)$, where $M_i \equiv \underline{M}(\text{mod } p_i)$, and $e_i \equiv e(\text{mod } p_i-1)$, and where i = 1, 2, . . . k.

52. (Currently amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding/decoding request provided with a plaintext/ciphertext message M/C to be encoded/decoded and with or without a public/private key that includes an exponent e/d and a modulus n representation of which exists in the memory in the form of its k distinct random prime number p_1, p_2, . . . p_k, where k ≥ 3,

obtaining the public/private key from the memory if the encoding/decoding request is provided without the public/private key,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values M_1, M_2, . . . M_k/C_1, C_2, . . . C_k, and

forming the ciphertext/plaintext message C/M from the subtask values C_1, C_2, . . . C_k/M_1, M_2, . . . M_k;

wherein p and q are a pair of prime numbers that product of which equals a modulus m, the k distinct random prime numbers each smaller than p

and q, and the modulus m having the same number of digits as the modulus n; and

wherein for a given number of digits for modulus n and modulus m, it takes fewer computational cycles to form the ciphertext/plaintext message C/M if the k distinct random prime numbers are used, relative to the number of computational cycles for forming a ciphertext/plaintext message C'/M' if the pair of prime numbers p and q is used instead.

53. (Previously presented) The system of claim 52 wherein when produced each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\text{mod } p_i)$, where $C_i \equiv C(\text{mod } p_i)$, and $e_i = e(\text{mod } p_i - 1)$, and where $i = 1, 2, \ldots, k$.

54. (Previously presented) The system of claim 52 wherein when produced each one of the subtasks $M_1, M_2, \ldots M_k$ is developed using a relationship of the form $M_i \equiv C_i^{d_i} (\text{mod } p_i)$, where $M_i \equiv M(\text{mod } p_i)$, and $d_i = d(\text{mod } p_i - 1)$, and where $i = 1, 2, \ldots, k$.

55. (Currently amended) The system of claim 54, wherein the private key exponent d relates to the public key exponent e [[vai]] via $d \equiv e^{-1}(\text{mod}((p_1 - 1)\cdot(p_2 - 1)\cdots(p_k - 1)))$.

56. (Currently amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime number $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, $p_1 - 1, p_2 - 1, \ldots p_k - 1$, is relatively prime to the public key portion e;

means for establishing a private key portion of d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for receiving a ciphertext message data C; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form

$$M \equiv C^d \pmod{n};$$

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein decoding said ciphertext message data C is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the decoding of said ciphertext message data C if the k distinct random prime numbers are used, relative to the number of computational cycles for performing a decoding of said ciphertext message data C if the pair of prime numbers p and q is used instead.

57. (Previously presented) The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

58. (Currently amended) A system for communications of a message cryptographically processed with RSA public key ~~encryption~~signing, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers p_1, p_2, . . . p_k, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion *e* of the form $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers: and

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s, using a relationship of the form

$$M_s \equiv M^d \ (\mathrm{mod}\ n),$$

where $0 \leq M \leq n-1$, the signed message M_s being decipherable using the public key portion e;

wherein p and q are a pair of prime numbers that product of which equals a composite number m, the k distinct random prime numbers each smaller than p and q, and the composite number m having the same number of digits as the composite number n;

wherein encoding said plaintext message data M is divided into sub-steps, one sub-step for each of the k distinct random prime numbers; and

wherein for a given number of digits for composite numbers n and m, it takes fewer computational cycles to perform the encoding of said plaintext message data M if the k distinct random prime numbers are used, relative to the number of computational cycles for performing an encoding of said plaintext message data M if the pair of prime numbers p and q is used instead.

59. (Currently amended) The system of claim 58 further comprising ~~the step of~~:

means for decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^{\,e} \pmod{n}$.

60. (Previously presented) The system of claim 57, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

61. (Previously presented) The system of claim 59, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key signing using a modulus value equal to n independent of the k distinct prime numbers.

62. (New) The method according to claim 14, wherein n and m include values that are more than 600 digits long.

63. (New) The method according to claim 16, wherein n and m include values that are more than 600 digits long.

64. (New) The method according to claim 18, wherein n and m include values that are more than 600 digits long.

65. (New) The method according to claim 20, wherein n and m include values that are more than 600 digits long.

66. (New) The method according to claim 22, wherein n and m include values that are more than 600 digits long.